National Nuclear Security Administration Orders Self-Study Program

Safety Basis Documentation

10 CFR 830, NUCLEAR SAFETY MANAGEMENT

DOE G 421.1-2, IMPLEMENTATION GUIDE FOR USE IN DEVELOPING DOCUMENTED SAFETY ANALYSES TO MEET SUBPART B OF 10 CFR 830

DOE G 423.1.1, IMPLEMENTATION GUIDE FOR USE IN DEVELOPING TECHNICAL SAFETY REQUIREMENTS

DOE G 424.1-1, IMPLEMENTATION GUIDE FOR USE IN ADDRESSING UNREVIEWED SAFETY QUESTION REQUIREMENTS

DOE-STD-1104-96, REVIEW AND APPROVAL OF NUCLEAR FACILITY SAFETY BASIS DOCUMENTS (DOCUMENTED SAFETY ANALYSES AND TECHNICAL SAFETY REQUIREMENTS)

NNSA
National Nuclear Security Administration

NNSA SERVICE CENTER

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

SAFETY BASIS DOCUMENTS
FAMILIAR LEVEL

OBJECTIVES

Given the familiar level of this module and the resources listed below, you will be able to:

1. State five general requirements for contractors who are responsible for a hazard category 1, 2, or 3 nuclear facility as related to establishing a safety basis.

2. State the actions a contractor must take when it is made aware of a potential inadequacy of the documented safety analysis.

3. State the three contractor requirements related to technical safety requirements (TSRs).

4. State the safe harbor methods used to prepare a documented safety analysis (DSA) for an NNSA nonreactor nuclear facility.

5. Discuss the purpose of a preliminary DSA for a new facility.

6. State the purpose of a final DSA.

7. State the three types of TSRs.

8. State the purpose of limiting conditions for operations.

9. State the purpose of action statements as used in TSRs.

10. State the purpose of an unreviewed safety question determination.

11. Discuss the approval basis for DSAs.

Note: If you think that you can complete the practice at the end of this level without working through the instructional material and/or the examples, complete the practice now. The course manager will check your work. You will need to complete the practice in this level successfully before taking the criterion test.

RESOURCES

10 CFR 830, "Nuclear Safety Management, Subpart B, Safety Basis Requirements"
DOE G 421.1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*.
DOE G 423.1-1, *Implementation Guide for Use in Developing Technical Safety Requirements*.
DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements.*
DOE-STD-1104-96, *Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements).*

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

INTRODUCTION

This module replaces the study guides for the following DOE Orders:

- DOE Order 5480.21, *Unreviewed Safety Questions*
- DOE Order 5480.22, *Technical Safety Requirements*
- DOE Order 5480.23, *Nuclear Safety Analysis Reports*

The familiar level of this module is divided into five sections. In the first section, we will discuss the regulation. In the second, third, and fourth sections, we will discuss the U. Department of Energy (DOE) guides for documented safety analyses (DSAs), technical safety requirements (TSRs), and unreviewed safety questions (USQs). Section 5 discusses the DOE standard related to DSAs and TSRs. We have provided several examples and practices throughout the module to help familiarize you with the material. The practices will also help prepare you for the criterion test.

Before continuing, you should obtain a copy of the references. You may need to refer to these documents to complete the examples, practices, and criterion test.

SECTION 1, 10 CFR 830, NUCLEAR SAFETY MANAGEMENT, SUBPART B, SAFETY BASIS REQUIREMENTS

The safety basis requirements of 10 CFR 830 require the contractor responsible for an NNSA nuclear facility to analyze the facility, the work to be performed, and the associated hazards; and to identify the conditions, safe boundaries, and hazard controls necessary to protect workers, the public, and the environment from adverse consequences. These analyses and hazard controls constitute the safety basis upon which the contractor and NNSA rely to conclude that the facility can be operated safely. Performing work consistent with the safety basis provides reasonable assurance of adequate protection of workers, the public, and the environment.

The safety basis requirements are intended to further the objective of making safety an integral part of how work is performed throughout the NNSA complex. Developing a thorough understanding of a nuclear facility, the work to be performed, the associated hazards, and the needed hazard controls is essential to integrating safety into management and work at all levels. Performing work according to the safety basis for a nuclear facility is the realization of that objective.

GENERAL REQUIREMENTS

The contractor responsible for a hazard category 1, 2, or 3 NNSA nuclear facility must establish and maintain the safety basis for the facility. In establishing the safety basis for a hazard category 1, 2, or 3 NNSA nuclear facility, the contractor responsible for the facility must

- define the scope of the work to be performed;
- identify and analyze the hazards associated with the work;
- categorize the facility in a manner consistent with DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance With DOE Order 5480.23, Nuclear Safety Analysis Reports;*
- prepare a documented safety analysis for the facility; and
- establish the hazard controls upon which the contractor will rely to ensure adequate protection of workers, the public, and the environment.

In maintaining the safety basis for a hazard category 1, 2, or 3 NNSA nuclear facility, the contractor responsible for the facility must

- update the safety basis to keep it current and to reflect changes in the facility, the work, and the hazards as they are analyzed in the DSA;
- submit either the updated DSA for approval or a letter stating that there have been no changes in the DS since the prior annual submission to NNSA, and
- incorporate any changes, conditions, or hazard controls directed by NNSA in the safety basis.

UNREVIEWED SAFETY QUESTION PROCESS REQUIREMENTS

The contractor responsible for a hazard category 1, 2, or 3 NNSA existing nuclear facility must submit for NNSA approval a procedure for its USQ process on a schedule that allows NNSA approval in a safety evaluation report.

The contractor must implement the NNSA-approved USQ procedure in situations where there is a

- temporary or permanent change in the facility as described in the existing documented safety analysis,
- temporary or permanent change in the procedures as described in the existing documented safety analysis,
- test or experiment not described in the existing documented safety analysis, or
- potential inadequacy of the documented safety analysis because the analysis may not be bounding or may be otherwise inadequate.

The contractor must obtain NNSA approval before taking any action that involves a USQ.

The contractor must annually submit a summary to NNSA of the USQ determinations performed since the prior submission.

If the contractor discovers or is made aware of a potential inadequacy of the documented safety analysis, it must

- take action, as appropriate, to place or maintain the facility in a safe condition until the safety of the situation is evaluated,
- notify NNSA of the situation,
- perform a USQ determination and notify NNSA promptly of the results; and
- submit the evaluation of the safety of the situation to NNSA before removing any operational restrictions.

DOCUMENTED SAFETY ANALYSIS REQUIREMENTS

The contractor responsible for a hazard category 1, 2, or 3 NNSA nuclear facility must obtain approval from NNSA for the methodology used to prepare the documented safety analysis.

The DSA for a hazard category 1, 2, or 3 NNSA nuclear facility must, as appropriate for the complexities and hazards associated with the facility:

- describe the facility, including the design of safety structures, systems, and components (SSC) and the work to be performed;

- provide a systematic identification of natural and man-made hazards associated with the facility;
- evaluate normal, abnormal, and accident conditions, including the consideration of natural and man-made external events, the identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and the consideration of the need for analysis of accidents that may be beyond the design basis of the facility;
- derive the hazard controls necessary to ensure adequate protection of workers, the public, and the environment; demonstrate the adequacy of these controls to eliminate, limit, or mitigate identified hazards; and define the process for maintaining the hazard controls current at all times and controlling their use;
- define the characteristics of the safety management programs necessary to ensure the safe operation of the facility, including quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, and radiation protection; and
- with respect to a nonreactor nuclear facility with fissionable material in a form and amount sufficient to pose a potential for criticality, define a criticality safety program that:
  - ensures that operations with fissionable material remain sub-critical under all normal and credible abnormal conditions,
  - identifies applicable nuclear criticality safety standards, and
  - describes how the program meets applicable nuclear criticality safety standards.

TECHNICAL SAFETY REQUIREMENTS

The contractor responsible for a hazard category 1, 2, or 3 NNSA nuclear facility must

- develop TSRs that are derived from the documented safety analysis;
- prior to use, obtain NNSA approval of TSRs and any changes to TSRs; and
- notify NNSA of any violation of a TSR.

The contractor may take emergency actions that depart from an approved TSR when no actions consistent with the TSR are immediately apparent, and when these actions are needed to protect workers, the public, or the environment from imminent and significant harm. Such actions must be approved by a certified operator for a reactor or by a person in authority as designated in the TSRs for nonreactor nuclear facilities. The contractor must report the emergency actions to NNSA as soon as practicable.

Note: You do not have to do Example 1 on the following pages, but it is a good time to check your skill and knowledge of the information covered. You may do Example 1 or go to Section 2.

Change No: 0
Safety Basis Documents
Level: Familiar
Date: 10/15/03

EXAMPLE 1

Using the familiar level of this module and the resources, complete the following exercises.

1. State in your words the purpose of 10 CFR 830, Subpart B, "Safety Basis Requirements."

2. State the requirements for maintaining a safety basis for an NNSA nuclear facility.

3. Discuss the purpose of DSAs.

Note: When you are finished, compare your answers to those contained in the Example 1

Self-Check. When you are satisfied with your answers, go to Section 2.

EXAMPLE 1 SELF-CHECK

1. State in your words the purpose of 10 CFR 830, subpart B, "Safety Basis Requirements."
   The safety basis requirements are intended to further the objective of making safety an integral part of how work is performed throughout the NNSA complex. Developing a thorough understanding of a nuclear facility, the work to be performed, the associated hazards and the needed hazard controls is essential to integrating safety into management and work at all levels. Performing work according to the safety basis for a nuclear facility is the realization of that objective.

2. State the requirements for maintaining a safety basis for an NNSA nuclear facility.
   The requirements for maintaining a safety basis are
   - update the safety basis to keep it current and to reflect changes in the facility, the work, and the hazards as they are analyzed in the DSA;
   - submit either the updated DSA for approval or a letter stating that there have been no changes in the DSA since the prior annual submission to NNSA, and
   - incorporate any changes, conditions, or hazard controls directed by NNSA in the safety basis.

3. Discuss the purpose of DSAs.
   A DSA demonstrates the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment.

Change No: 0
Safety Basis Documents
Level: Familiar
Date: 10/15/03

SECTION 2, DOE G 421.1-2, IMPLEMENTATION GUIDE FOR USE IN DEVELOPING DOCUMENTED SAFETY ANALYSES TO MEET SUBPART B OF 10 CFR 830

This guide describes suggested non-mandatory approaches for meeting requirements in 10 CFR 830 related to developing DSAs. Accelerators and their operations are excluded from the safety basis requirements of the rule because their activities normally do not use, store, or form radioactive materials. However, target areas associated with the accelerators and areas associated with the radioactive materials produced by the accelerators are not considered to be part of the accelerator and continue to be subject to the provisions of 10 CFR 830 to the extent that they use, store, or form radioactive materials. Thus, target areas that contain or form radioactive inventories within the DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance With DOE Order 5480.23, Nuclear Safety Analysis Reports*, section 2 limits are subject to 10 CFR 830.

The preparation of DSAs must conform to one of the methods set forth in table 1 or an alternate method approved by NNSA. These methods are called safe harbors in 10 CFR 830. The use of alternative methods or significant deviations from the safe harbor methods, if proposed, must be approved by the responsible NNSA organization as defined in DOE M 411.1-1B, *Safety Management Functions, Responsibilities, and Authorities Manual*, including the concurrence of the Office of Environment, Safety, and Health.

Table 1. Safe Harbor Methods for DSAs.

The contractor responsible for:	may prepare its documented safety analyses by:
(1) a DOE reactor	using the method in U.S. Nuclear Regulatory Commission Regulatory Guide 1.70, *Standard Format and Content of Safety Analysis Reports for Nuclear Power Plants*, or successor document.
(2) a DOE nonreactor nuclear facility	using the method in DOE-STD-3009-94, Change Notice No. 1, January 2000, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*, dated July 1994, or successor document.
(3) a DOE nuclear facility with a limited operational life[2]	using the method in either: (1) DOE-STD-3009-94, Change Notice No. 1, dated January 2000, or successor document, or (2) DOE-STD-3011-94, *Guidance for Preparation of DOE 5480.22 (TSR) and DOE 5480.23 (SAR) Implementation Plans*, dated November 1994, or successor document.
(4) the deactivation or the transition surveillance and maintenance of a DOE nuclear facility	using the method in either: (1) DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document, or (2) DOE-STD-3011-94 or successor document.
(5) the decommissioning of a DOE nuclear facility	(1) using the method in DOE-STD-1120-98, *Integration of Environment, Safety, and Health into Facility Disposition Activities*, dated May 1998, or successor document; (2) using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing safety and health programs, work plans, health and safety plans (HASPs), and emergency response plans to address public safety, as well as worker safety; and (3) deriving hazard controls based on the safety and health programs, the work plans, the HASPs, and the emergency response plans.
(6) a DOE environmental restoration activity that involves either work not done within a permanent structure or the decommissioning of a facility with only low-level residual fixed radioactivity.	(1) using the method in DOE-STD-1120-98 or successor document, and (2) using the provisions in 29 CFR 1910.120 (or 29 CFR 1926.65 for construction activities) for developing a safety and health program and a site-specific HASP (including elements for emergency response plans, conduct of operations, training and qualifications, and maintenance management).

Table 1. Safe Harbor Methods for DSAs (continued).

The contractor responsible for:	**may prepare its documented safety analyses by:**
(7) a DOE nuclear explosive facility and the nuclear explosive operations conducted therein	developing its DSA in two pieces: (1) a safety analysis report for the nuclear facility that considers the generic nuclear explosive operations and is prepared in accordance with DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document, and (2) a hazard analysis report for the specific nuclear explosive operations prepared in accordance with DOE-STD-3016-99, *Hazards Analysis Reports for Nuclear Explosive Operations*, dated February 1999, or successor document.
(8) a DOE Hazard Category 3 nonreactor nuclear facility	using the methods in Chapters 2, 3, 4, and 5 of DOE-STD-3009, Change Notice No. 1, dated January 2000, or successor document to address in a simplified fashion: (1) the basic description of the facility/activity and its operations, including safety SSCs; (2) a qualitative hazards analysis; and (3) the hazard controls (consisting primarily of inventory limits and safety management programs) and their bases.
(9) transportation activities	(1) preparing a safety analysis report for packaging in accordance with DOE O 460.1A, *Packaging and Transportation Safety*, or successor document and (2) preparing a transportation safety document in accordance with DOE G 460.1-1, *Implementation Guide for Use with DOE O 460.1A, Packaging and Transportation Safety*, dated 6-5-97, or successor document.
(10) transportation and onsite transfer of nuclear explosives, nuclear components, Naval nuclear fuel elements, Category I and Category II special nuclear materials, special assemblies, and other materials of national security	(1) preparing a safety analysis report for packaging in accordance with DOE O 461.1, *Packaging and Transportation of Materials of National Security Interest*, dated 9-29-00, or successor document and (2) preparing a transportation safety document in accordance with DOE M 461.1-1, *Packaging and Transfer of Materials of National Security Interest Manual*, dated 9-29-00, or successor document.

Development of a DSA or preliminary documented safety analysis (PDSA) is the process whereby facility hazards are identified, controls to prevent and mitigate potential accidents involving those hazards are proposed, and commitments are made for design, construction, operation, and disposition so as to ensure adequate safety at NNSA nuclear facilities. NNSA, in its review and approval role, may require modification or addition to these commitments by the responsible contractor. Throughout the life of the facility, from design and construction to mission-oriented operations, through deactivation, long-term surveillance and maintenance, to decontamination and decommissioning, there must be a safety basis in place that is appropriate to the activities (operations) occurring during each of those phases.

During design and construction, the governing safety basis document is the PDSA. It is updated as the design matures and is approved before procurement and construction activities. Until approval, the PDSA and its updates tell NNSA how nuclear safety design criteria are being addressed in the design. Project design reviews provide the vehicle by which safety-related changes are reviewed and NNSA can provide guidance to the contractor. Before operations, the PDSA evolves to a final DSA that reflects the facility as actually constructed.

During mission-oriented operations and for each phase thereafter until the facility falls below the category 3 threshold for nuclear facilities, the DSA must be kept current, considering any changes to the facility or its operations. The USQ process is key to this requirement. The USQ process must be integrated with the configuration management process that must be a part of the safety management program commitments of a DSA. The USQ process is the tool by which it is determined when NNSA must approve any changes to the facility or its operations.

A DSA must demonstrate the extent to which a nuclear facility can be operated safely with respect to workers, the public, and the environment. NNSA expects a contractor to use a graded approach to develop a DSA and describe how the graded approach was applied. The level of detail, analysis, and documentation will reflect the complexity and hazard associated with a particular facility or activity. Thus, the DSA for a simple, low-hazard facility may be relatively short and qualitative in nature, while the DSA for a complex, high-hazard facility may be quite elaborate and quantitative. NNSA will work with its contractors to ensure a DSA is appropriate for the facility or activity for which it is being developed.

DSAs are designed to be the primary reference on facility safety. Contractor management uses the DSAs for new nuclear facilities, to have an authoritative documented record of DSA derived and programmatic safety commitments made to NNSA governing safety and health aspects of project management, engineering, design, procurement and construction of the facility or the development of the nuclear operation. DOE O 420.1, *Facility Safety*, contains requirements for the design of new nuclear facilities and mandates the use of safety analyses to guide safety aspects of design. Additionally, 10 CFR 835, subpart K, "Occupational Radiation Protection," contains regulatory requirements for design and control. These analyses should be summarized in the DSA to support the rationale for safety aspects of design.

PRELIMINARY DOCUMENTED SAFETY ANALYSIS

To obtain early agreement between NNSA and its contractors regarding what safety systems and design features are needed in new nuclear facilities, a contractor responsible for a new DOE nuclear facility or a major modification to an existing DOE nuclear facility that is hazard category 1, 2, or 3 must submit a PDSA to NNSA for approval. NNSA approves the PDSA before procuring materials or components, or beginning construction.

PDSAs for new facilities serve as the principal safety basis for the NNSA decision to authorize design, procurement, construction, and pre-operational testing. The safety analysis should be initiated and technical interchanges conducted with NNSA at the earliest practical point in conceptual or preliminary design. The PDSA will identify preliminary commitments to the facility's ultimate design and operation.

NNSA does not expect a PDSA for activities that do not involve significant construction or for activities that are not major modifications. For activities that are not major modifications, the USQ process should be used to determine if NNSA approval is needed. If so, a safety analysis that supports the request for approval should be developed. If the request is approved, then the safety analysis should be included in the DSA when the modification is completed.

The PDSA required by 10 CFR 830.206, “Unreviewed Safety Question Process,” may need updating to sustain the reliability of the information until it is superseded by a Final DSA.

A PDSA should contain a description of

- the preliminary design of the facility with respect to safety systems and safety design features,
- research or other data collection necessary to finalize the design, and
- the preliminary approaches to startup and operations management.

The PDSA should show how the nuclear safety design criteria will be satisfied. Additionally, a PDSA should contain descriptions and commitments to NNSA with respect to contractor management and oversight of the construction project.

Table 2 in DOE G 421.1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830,* summarizes the PDSA development process for capital acquisition projects in relation to project milestones. Such projects would include new facilities and major additions to existing facilities. The rule requires a PDSA for major modifications and defines a major modification as substantial changes to the safety basis of a facility.

FINAL DOCUMENTED SAFETY ANALYSIS

During construction, the final DSA is developed. It is based on the facility as built and as it will be operated and finalizes the description of needed safety management programs. After the construction has been completed and the DSA has been updated to reflect the as-built design and development of the TSR bases, NNSA reviews the revised DSA and updates the safety evaluation report authorizing operations subject to any necessary conditions, including the need for an operational readiness review. Approved final DSAs, TSRs, and other hazard control documents contain the principal safety basis for an NNSA decision to authorize facility operation. Once facility operation is authorized, the final DSA and hazard controls will be the principal safety basis for sustaining authorization and safety oversight.

A final DSA documents the safety basis and provides detailed information for a determination that the facility can be operated, maintained, shut down, and decommissioned safely and in compliance with applicable laws and regulations. Contractors must ensure that information in a DSA is current and applicable. When a facility changes status from a production-oriented status to inactive, the DSA and TSR associated with the facility or activity must be updated to describe the activities, consider the hazards associated with the new status, and identify the controls associated with these hazards. Any facility or activity DSA that does not reflect its current status is out of compliance with the safety basis rule. The annual update required by the rule applies to all DSAs, including those not yet rule compliant. NNSA remains accountable for safety during the period those DSAs are being upgraded.

Note: You do not have to do Example 2 on the following page, but it is a good time to check your skill and knowledge of the information covered. You may do Example 2 or go to Section 3.

EXAMPLE 2

1. State the safe harbor method for preparing a DSA for a nonreactor nuclear facility.

2. State the contents of a PDSA.

3. When is a DSA update required?

Note: When you are finished, compare your answers to those contained in the Example 2 Self-Check. When you are satisfied with your answers, go on to Section 3.

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

EXAMPLE 2 SELF-CHECK

1. State the safe harbor method for preparing a DSA for a nonreactor nuclear facility.
   Use the method in DOE-STD-3009-94, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Safety Analysis Reports*.

2. State the contents of a PDSA.
   A PDSA should contain a description of the preliminary design of the facility with respect to safety systems and safety design features, identify research or other data collection necessary to finalize the design, and document the preliminary approaches to startup and operations management. The PDSA should show how the nuclear safety design criteria will be satisfied. A PDSA should also contain descriptions and commitments to NNSA with respect to contractor management and oversight of the construction project.

3. When is a DSA update required?
   Annually or when a facility encounters changes that affect the safety basis.

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

SECTION 3, DOE G 423.1-1 IMPLEMENTATION GUIDE FOR USE IN DEVELOPING TECHNICAL SAFETY REQUIREMENTS

TSRs define the performance requirements of safety SSCs and identify the safety management programs that ensure safety. TSRs are aimed at confirming the ability of the SSCs and personnel to perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analyses of the activities and through identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs.

Through analyses of the encompassing bounding accidents, the necessary safety systems and accident mitigating systems are identified and their characteristics are defined. Flowing from the analyses is information that provides the basis for controls, limits, and conditions for operation, known as TSRs. TSRs explicitly show this relationship. The content of the DSA must remain valid so that the safety basis of the facility, as implemented in operations through the TSR, remains valid. Therefore, there is a commitment to the process of USQs regarding any proposed change to the facility or its operations as described in the DSA. Likewise, all changes to the TSR basis presented in the DSA should be incorporated into the TSRs to ensure the information reflects the current safety basis of the facility.

Any proposed revision to a TSR should be examined to ensure the basis for the change is supported in the DSA. The TSR rule requires that such revisions be submitted to NNSA for review with the basis for the proposed change. The change to the TSR must be approved by NNSA before it is implemented.

TECHNICAL SAFETY REQUIREMENT LIMITS

There are three types of TSR limits: safety limits (SLs), limiting control settings (LCSs), and limiting conditions for operations (LCOs). The intent of these limits is to ensure that the operating regime is restricted to the bounds of safe operation as defined by the safety analyses.

Safety Limits

SLs are limits on important process variables that are needed for the facility function. If SLs are exceeded, it could directly cause the failure of one or more of the passive barriers that prevent the uncontrolled release of radioactive materials. SL designation is distinct to process events because other events, such as external or natural phenomena events, that may also challenge the passive safety boundary have no SLs because they are not under operator control.

Generally, containment/confinement should not be considered as barriers that require SLs because they are mitigative in nature. However, these systems should be considered in the development of LCOs.

For nonreactor nuclear facilities, the passive barriers preventing the uncontrolled release of radioactive and other hazardous materials are the process material boundaries closest to the source. Failure must be immediate and catastrophic upon reaching the failure value as opposed to a long-term degradation failure such as by wall thinning, chemical corrosion, etc. Limits of importance for non-reactor nuclear facilities are facility specific, but could relate to pressure, combustible/flammable material limits, and process heat-up limits.

Limiting Control Settings

LCSs define the settings on safety systems that control process variables to prevent exceeding an SL.

LCSs of instruments that monitor process variables at nonreactor nuclear facilities are the settings that either initiate protective devices themselves or sound an alarm to alert facility personnel to take action to protect barriers that prevent the uncontrolled release of radioactive materials. An LCS is only specified for a variable that also protects an SL. LCSs should be chosen so that there is adequate time after exceeding the setting to correct the abnormal situation automatically or manually before an SL is exceeded.

In general, each item requiring an SL will also have control or alarm settings to ensure that the SL is not violated. However, only those control or alarm settings that are relied on in the safety analysis would become LCSs in the TSR.

When developing TSR limiting values or set points based on the DSA, remember the values in the DSA are generally the exact values at which something is assumed to happen. The values and set points in the TSR are measured, so the DSA values must be adjusted before use in the TSR to ensure that the action assumed in the DSA actually occurs on the conservative side of the DSA assumptions. The adjustments should account for: calibration uncertainty, instrumentation uncertainty during operation, instrument drift, and instrument uncertainty during accident conditions

Limiting Conditions for Operations

LCOs define the limits that represent the lowest functional capability or performance level of safety SSCs required to perform an activity safely. LCOs should include the initial conditions for those design basis accidents or transient analyses that involve the assumed failure of, or present a challenge to, the integrity of the primary radioactive material barrier. Identification of these variables should come from a search of each transient and accident analysis documented in the DSA. The LCO should be established at a level that will ensure the process variable is not less conservative during actual operation than was assumed in the safety analyses. LCOs should also include those SSCs that are part of the primary success path of a safety sequence analysis and those support and actuation systems necessary for them to function successfully. Support equipment for these SSCs would normally be part of the LCO if relied on to support the SSCs function.

The primary success path of a safety sequence analysis is the sequence of events assumed by the safety analyses that leads to the conclusion of a transient or accident with consequences that are acceptable. Hence, any SSC providing a safety function in that assumed sequence should be included in the LCOs. Each transient or accident analysis that challenges the integrity of a radioactive material barrier, or involves its assumed failure, should be studied to compile a list of involved SSCs.

When an LCO is not met, action should be initiated within one hour to place the facility in a mode in which the requirement does not apply. However, note that at nonreactor nuclear facilities, the LCOs that provide for monitoring for a breach of the barriers containing radioactive material are applicable in all modes. The action statement in this case should be rapid restoration of the capability, or compensatory measures. Entry into a different mode should not be made unless all of the LCOs are met for that mode, except for the passage through a mode as required to comply with action statements.

Action Statements

Action statements should describe the actions to be taken in the event that an operating limit is not met. An action statement should establish the steps and time limits to correct the condition or conditions that are beyond the TSR limits.

The action statement for LCOs should state the action required to address the condition that does not meet the LCO. Normally, this simply requires that the adverse condition be corrected in a certain time frame and provides further action if this is impossible. For example, if an LCO requires two pumps at all times when in the operation mode, the action statement would likely state that if one pump is inoperable it should be made operable in X hours or the facility should be placed in warm standby mode within the following Y hours. If both pumps were inoperable, the action statement would likely require at least one pump be operable in Z hours and the second pump operable in the following W hours or the facility should be placed in warm standby mode.

An action statement should provide a safe and unambiguous method to reach a safe, stable state. However, for complex facilities, considerable care should be exercised to ensure that an action statement does not unacceptably decrease safety. Thus, action statements should avoid causing a loss of safety function either directly or by making support systems inoperable.

Occasionally, it may be necessary for an action statement to specify transition through an operating mode even though required safety equipment would be inoperable. For such cases the transition condition should be carefully evaluated to ensure that the facility’s risk is not increased by the action statement.

The action statement for nuclear criticality safety LCOs should normally specify that the process or activities not in compliance with the LCO should be stopped immediately (if this action would not result in a less stable condition) and the process, system, or area be restored to a safe condition according to an approved recovery plan.

Operability

Operability embodies the principle that a system can perform its safety function only if all necessary support systems are capable of performing their related support functions. This definition extends the requirements of an LCO for those systems that directly perform a specified safety function (supported systems) to those that perform a required support function (support systems).

A system or component can be degraded but still operable if it remains capable of performing its required safety function at the level assumed in the accident analysis. If systems are functioning but under stress, judgment must be used concerning a declaration of inoperability.

General principles of operability should be followed in generating LCOs.

General Principle 1
A system is considered operable as long as there is assurance that it is capable of performing its specified safety function(s).

General Principle 2
A system can perform its specified safety function(s) only when all of its necessary support systems are capable of performing their related support functions.

General Principle 3
When all systems designed to perform a certain safety function are not capable of performing that safety function, a loss of function condition exists.

General Principle 4
When a system is incapable of performing its intended safety function(s), the declaration of inoperability should be immediate.

Surveillance Requirements

Surveillance requirements (SRs) are used to ensure operability or availability of the safety SSCs identified in the operating limits (OLs). SRs are most often used with LCOs to periodically validate the operability of active systems or components that are subject to a limiting condition.

SRs consist of short descriptions of the type of surveillance required and its frequency of performance. These statements should be as brief as possible but should identify those requirements needed to ensure compliance with the related OLs. Each SR should begin with a verb. Use of terms and sentence structure among requirements should be consistent.

Administrative Controls

Administrative controls (ACs) are the provisions relating to organization and management, procedures, record keeping, reviews, and audits necessary to ensure safe operation of the facility. ACs may include reporting deviations from TSRs or staffing requirements for facility positions important to safe operation of the facility.

Violation of Technical Safety Requirements

Although the TSR elements have an importance hierarchy, a TSR violation can occur for each type of TSR. Violations of a TSR occur as a result of the following four circumstances:

- exceeding an SL
- failure to complete an action statement within the required time limit following exceeding an LCS or failing to comply with an LCO
- failure to perform a surveillance within the required time limit
- failure to comply with an AC statement

Failure to comply with an AC statement is a TSR violation when either the AC is directly violated or the intent of a referenced program is not fulfilled. To qualify as a TSR violation, the failure to meet the intent of the referenced program would need to be significant enough to render the DSA summary invalid.

TSR violations involving SLs require the facility to begin immediately to go to the most stable, safe condition attainable, including total shutdown.

A grace period is sometimes provided to perform a missed surveillance, thereby avoiding the need for a facility to take immediate, possibly unnecessary corrective action. Entering the grace period remains a TSR violation even though an immediate corrective action may not be required.

Safety Structures, Systems, and Components

Safety-class SSCs are those items relied on to ensure the safety and health of the public. This may include radiation monitoring equipment and alarms. The distinction between what is safety-class and what is not is made by the DSA or by other safety documentation. In general, safety-class SSCs should have one or more associated TSRs to ensure performance of their safety function.

Systems that are identified in the DSA as operating and performing a safety function that is required to meet additional DSA safety criteria also need TSRs. Support systems for safety-class SSCs would normally be considered safety-class if they are relied on to support a safety-class function.

Each safety-class SSC should have a corresponding TSR. SLs are, by definition, associated with passive physical barriers that prevent the release of radioactive materials. Passive safety-class systems and components, even those associated with an SL, will generally be listed in the design features as opposed to LCOs. Active safety-class systems and components will generally have associated LCOs to ensure operability. All of the SSCs may have surveillance and maintenance requirements depending on their function and characteristics.

Note: You do not have to do Example 3 on the following page, but it is a good time to check your skill and knowledge of the information covered. You may do Example 3 or go directly to Section 4.

EXAMPLE 3

1. State the purpose of TSRs.

2. Define the term “safety limits.”

3. Define the term “limiting conditions for operations.”

Note: When you are finished, compare your answers to those contained in the Example 3 Self-Check. When you are satisfied with your answers, go on to Section 4.

EXAMPLE 3 SELF-CHECK

1. State the purpose of TSRs.
   TSRs define the performance requirements of safety SSCs and identify the safety management programs that ensure safety.

2. Define the term "safety limits."
   SLs are limits on important process variables that are needed for the facility function.

3. Define the term "limiting conditions for operations."
   LCOs define the limits that represent the lowest functional capability or performance level of safety SSCs required to perform an activity safely.

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

SECTION 4, DOE G 424.1-1, IMPLEMENTATION GUIDE FOR USE IN ADDRESSING UNREVIEWED SAFETY QUESTION REQUIREMENTS

INTRODUCTION

The USQ process allows contractors to make physical and procedural changes and to conduct tests and experiments without prior NNSA approval if the proposed change can be accommodated within the existing safety basis. The contractor must evaluate any proposed change to ensure that it will not affect the safety basis of the facility. 10 CFR 830.203, "Unreviewed Safety Question Process," requires NNSA approval of the procedure to implement the USQ process.

Contractors should implement procedures to ensure that proposed changes to physical characteristics or operating procedures are adequately evaluated relative to the approved safety basis. Those proposed changes that involve USQs are brought to the attention of NNSA for review and approval before changes are made. A proposed change or test involves a USQ if

- the probability or consequences of an accident or malfunction of equipment important to safety could be increased,
- the possibility of a different type of accident than previously evaluated in the DSA could be introduced, or
- margins of safety could be reduced.

The existence of a USQ does not mean that the facility or operation is unsafe. The purpose of the USQ process is to alert NNSA of events, conditions, or actions that affect the NNSA-approved safety basis of the facility or operation and ensure appropriate NNSA line management action. If a change is proposed or a condition is discovered that could increase the risk of operating a facility beyond that established in the current safety basis, NNSA line management must review and determine the acceptability of that risk through the process of approving a revised safety basis that the contractor would develop and submit.

USQ APPLICATION

USQs apply to all category 1, 2, and 3 nuclear facilities. USQ determinations are required for changes to a nuclear facility that alter an SSC's design, function, or method of performance as described in the existing safety analyses by text, drawing, or other information relied on as the safety basis.

A USQ determination may have to be prepared for changes to procedures that are identified in the facility DSA. Procedures are not limited to those items specifically identified as procedure types but could include anything described in the DSA that defines or describes activities or controls over the conduct of work. Changes to these activities or controls qualify as changes to procedures as described in the DSA, and therefore must be evaluated as a potential USQ.

Changes to procedures include revising an existing procedure and creating a new procedure. For the case of a new procedure the question is, if the DSA were to be prepared after the new procedure had been approved, is the new procedure a type that would be identified in the DSA? If so, a USQ determination should be prepared for the new procedure.

Written USQ determinations are required for tests or experiments not described in the existing safety analyses. Tests and experiments should be broadly interpreted to include new activities or operations. By definition, these are activities that could degrade the margins of safety during normal operations or anticipated transients or degrade the ability of SSCs to prevent accidents or mitigate accident conditions.

Written USQ determinations are required when a contractor identifies a potential inadequacy of the safety analyses that support the NNSA-approved safety basis. Because an inadequacy in the safety analyses has the potential to call into question information relied on for authorization of operations, NNSA requires that the contractor

- take appropriate action to place or maintain the facility in a safe condition,
- notify NNSA when the information is discovered,
- perform a USQ determination and submit the results promptly, and

- complete an evaluation of the safety of the situation and submit it to NNSA before removing any operational restrictions that are implemented to compensate for the analytical discrepancy.

USQ IMPLEMENTATION

The USQ review process should be integrated into all technical aspects of the contractor organization responsible for design, engineering, maintenance, inspection, operations, and assessment of the nuclear facility or activity.

The USQ process should be implemented with a change control process that includes generalized steps for

- identifying and describing the temporary or permanent change,
- reviewing the technical aspects of the change,
- reviewing and approving the change,
- implementing the change, and
- documenting the change.

Contractors should develop procedures that provide detailed guidance for the performance of the USQ process, including any screening and the USQ determinations. The procedures should

- define the purpose of the procedure;
- set forth the procedure's applicability;
- provide definitions of appropriate terms, include screening criteria, as appropriate, and the basis for their application;
- include detailed guidance on what must be considered and evaluated when performing or reviewing a USQ determination;
- define the qualifications needed and responsibilities of personnel performing and reviewing USQ determinations; and
- include documentation requirements for each USQ determination.

USQ DETERMINATIONS

A USQ determination is that record required to document the review of a change or a situation where there is reason to believe that the facility's existing safety analysis may be in error or otherwise inadequate. For the purpose of USQ procedures and performing USQ determinations, the three USQ criteria should be broken down into seven questions:

1. Could the proposed change increase the probability of an accident previously evaluated in the facility's existing safety analyses?
2. Could the proposed change increase the consequences (to workers or the public) of an accident previously evaluated in the facility's existing safety analyses?
3. Could the proposed change increase the probability of a malfunction of equipment important to safety previously described in the facility's existing safety analyses?
4. Could the proposed change increase the consequences of a malfunction of equipment important to safety described in the facility's existing safety analyses?
5. Could the proposed change create the possibility of an accident of a different type than any previously evaluated in the facility's existing safety analyses?
6. Could the proposed change create the possibility of a malfunction of equipment important to safety of a different type than any previously evaluated in the facility's existing safety analyses?
7. Does the proposed change reduce the margin of safety?

The contractor must retain records of USQ actions for at least the full operational lifetime of the facility, until the facility is turned over to the decommissioning and decontamination phase.

Implementing procedures should establish the personnel training and qualifications needed to perform the USQ process. These include required educational background, years and/or types of work experience, knowledge of the facility, understanding NNSA requirements related to the facility safety basis, and familiarity with the facility-specific safety basis. All personnel responsible for preparing, reviewing, or approving USQ documents should receive training on the application of Section 830.203, including any facility-specific procedures. The recommended interval for retraining is every two years. The contractor should maintain a list of those personnel who are currently qualified to perform the USQ process.

Section 5, DOE-STD-1104-96, Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements)

INTRODUCTION

Safety and health assurance may be increased by standardizing the process of reviewing and approving DSAs and TSRs. Certain benefits are gained by standardizing fundamental elements of the review and approval process. To that end, this standard establishes NNSA guidelines for the review and approval of these documents, including preparation of safety evaluation reports (SERs), for nuclear facilities.

The body of this standard focuses on management of the review and approval process, provides guidelines for establishing the basis of approval, and recommends a format and content for SERs.

PLANNING

A review plan defines the extent and details of the review process for each DSA. Plans should be developed before the DSA is submitted for approval. The plan should be approved by the approval authority with a copy forwarded to the facility contractor for their information. Basic components of a review plan include

- scope and objectives of the review and their bases, including technical-, mission-, and/or project-related influences impacting the extent and methodology of the review, including basic task identification, objectives, and criteria by which the review is to be conducted;
- resources required for the review;
- process and requirements for providing orientation for the reviewers;
- means of coordinating the review;
- required SER reviews and signoffs; and
- schedule for the review, including key milestones for the review process.

An important part of planning is selecting the individuals for the review team. Members of the review team are typically selected based on technical qualifications, experience, familiarity with the subject matter, independence from preparation of the DSA, understanding of NNSA's safety assurance strategy, and availability. The review team requires a core team with expertise in process hazards analysis and accident analysis. The core of the review effort is assessing the hazard and accident analysis in the DSA because these analyses are the primary sources of original material with which the remainder of the DSA is aligned. Other personnel with diverse experience in safety and health and facility operations are not necessarily members of the core team but collectively provide support as needed for a thorough assessment of the facility safety basis. The extent of support necessary is reflected by the hazard and complexity level of the activities being examined.

Reviewers are required to justify the safety significance of an issue through substantiation of its impact on the safety basis if left unresolved. Each significant issue submitted should be accompanied by justification for its significance. The review team leader, and subsequently the approval authority, rely on these justifications in determining the relevance of all issues.

A significant issue identifies a problem or concern that affects the utility or validity of the safety basis documentation. Such issues are generally those involving

- hazardous material or energy release with significant consequences to the public, worker, or environment that will otherwise be left without coverage in the DSA;
- technical errors that invalidate major conclusions relevant to the safety basis; or
- failure to cover topical material required by NNSA regulations, directives, and guidance on DSAs.

If thorough justification of the significance of an issue is not provided and supported, the review team leader may determine that the issue is not significant. Such judgments may be appealed to the approving authority. While only significant issues require formal resolution, the review team leader will typically transmit all issues to the DSA preparer that will improve overall preparation of the DSA. The preparer may resolve these issues without formal response. The objective is not to document a large number of issues but to improve the DSA.

The preparer develops resolutions for significant issues and submits them to the review team leader. The review team leader forwards the proposed resolutions to the reviewers who originated the issues. The reviewers may respond if a resolution is considered unsatisfactory. All responses are transmitted through the review team leader, who schedules and arbitrates the process of resolution.

The review team leader may consider proposed resolutions satisfactory in the absence of timely responses or adequate justification of unacceptability by the issue originator. The review team leader ensures that the preparer is formally notified of acceptable and unacceptable resolutions that are proposed for significant issues.

Reviewers or the preparer of the DSA may appeal the disposition of an issue by the review team leader to the approval authority. The approval authority determines the final disposition of issues as it is the ultimate responsibility of the approval authority to achieve a defensible position for the final product. Neither a reviewer nor the preparer has veto power over ultimate resolution or disposition of an issue and neither need be satisfied with the final resolution. The review team leader ensures that final disposition of significant issues is documented, including minority opinions and dissenting views.

APPROVAL BASIS FOR DOCUMENTED SAFETY ANALYSES

NNSA evaluates the DSA by considering the extent to which the DSA adequately addresses the criteria set forth in 10 CFR 830.202, “Safety Basis” and 10 CFR 830.204, “Documented Safety Analyses” and satisfies the provisions of the methodology used to prepare the DSA. DSA review and approval focus on the adequacy of the following approval bases

- base information;
- hazard and accident analyses;
- safety SSCs;
- derivation of TSRs; and
- safety management program characteristics.

Base Information

Base information is the part of the approval basis that should be reviewed first. Base information includes elements of DSA preparation, completeness, and general content. Base information is not reviewed for accuracy but for sufficiency to allow assessment of the other approval bases that rely on this information. The review for sufficiency can range from a simple screening effort to more detailed discussions, depending on the complexity of the DSA.

Insufficient or incomplete base information in a DSA may prevent further review of the DSA. Reviewers should require resolution of major discrepancies in base information before evaluating the more specific aspects of the safety basis. Determining the adequacy of base information entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The facility contractor development and approval processes demonstrate sufficient commitment to establish the facility safety basis.
- The facility mission(s) and scope of operations for which safety basis approval is being sought are clearly stated and reflected in the type and scope of operations analyzed in the DSA.
- A description of the facility's life-cycle stage, mission(s), scope of operations, and the design of safety SSCs is presented, including explanation of the impact on the facility safety basis.
- A clear basis for and provisions of exemptions, consent agreements, and open issues is presented.
- A description of the site, facility, and operational processes provides sufficient background material to understand the major elements of the safety analysis.
- A correlation is established between actual facility arrangements and operations with those stated in the DSA. This may be accomplished successfully through reference to facility walkthroughs during DSA preparation. Walkthroughs may also be warranted during DSA review to provide some level of assurance that the actual physical arrangement of a facility corresponds to what is documented in the DSA.

Hazard and Accident Analyses

Another of the DSA approval bases is hazard and accident analyses. Hazard and accident analyses form the foundation for the remaining approval bases. Determining the adequacy of hazard and accident analyses entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The hazard analysis includes hazard identification that specifies or estimates the hazards relevant for DSA consideration in terms of type, quantity, and form, and also includes properly performed facility hazard categorization.
- The final hazard category for the facility is consistent with DOE-STD-1027, *Hazard Categorization and Accident Analysis Techniques For Compliance With DOE Order 5480.23, Nuclear Safety Analysis Reports*, section 2, change notice 1. Any differences between the final hazard category and the initial hazard category are explained.
- The hazard analysis includes a hazard evaluation that covers the activities for which approval is sought, is consistent in approach with safe harbor methods, identifies preventive and mitigative features for the spectrum of events examined, and identifies dominant accident scenarios through ranking.
- The hazard analysis evaluates normal, abnormal, and accident conditions, including consideration of natural and man-made external events, identification of energy sources or processes that might contribute to the generation or uncontrolled release of radioactive and other hazardous materials, and consideration of the need for analysis of accidents that may be beyond the design basis of the facility.
- The hazard analysis results are clearly characterized in terms of public safety, defense in depth, worker safety, and environmental protection.
- Subsequent accident analysis clearly substantiates the findings and descriptions of hazard analysis for the subset of events examined and confirms their potential consequences. Events potentially exceeding evaluation guidelines need to clearly identify associated safety-class SSCs and the basis of any TSR deviations.

Safety Structures, Systems, and Components

The next DSA approval basis is SSCs. Identification of safety SSCs is a product of the hazard and accident analyses. Determining the adequacy of safety SSCs entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The safety SSCs identified and described are consistent with the logic presented in the hazard and accident analyses.
- Safety functions for safety SSCs are defined with clarity and are consistent with the basis derived in the hazard and accident analyses.

- Functional requirements and system evaluations are derived from the safety functions and provide evidence that the safety functions can be performed.
- Control of safety SSCs relevant to TSR development is clearly defined.

Derivation of Technical Safety Requirements

Derivation of TSRs is the next DSA approval basis. Hazard controls are derived to eliminate, limit, or mitigate hazards and are generally safety SSCs or commitments to safety management programs, which are ultimately included in TSRs. Identification of TSRs results from the most significant preventive and mitigative features identified in the hazard and accident analyses and from the designation of safety SSCs. Determining the adequacy of the derivation of TSRs entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- TSRs are identified to ensure adequate protection of workers, the public, and the environment.
- The bases for deriving TSRs, that are identified and described in the hazard and accident analyses and safety SSC chapters, are consistent with the logic and assumptions presented in the analyses.
- The bases for deriving SLs, LCSs, LCOs, SRs, and ACs are appropriate.
- The process for maintaining the TSRs current at all times and for controlling their use is defined.

Safety Management Program Characteristics

Safety management program characteristics is the last DSA approval basis and includes the elements of institutional programs and facility management that are necessary to ensure safe operations based on assumptions made in the hazard and accident analyses. While these elements must be addressed in the DSA, generic descriptions of these institutional programs should not be duplicated in the DSA if they can be referenced in integrated safety management system documents or site-wide manuals. These institutional programs include quality assurance, procedures, maintenance, personnel training, conduct of operations, emergency preparedness, fire protection, waste management, radiation protection, and criticality safety. Identification of safety management program characteristics is a product of hazard and accident analyses, designation of safety SSCs, and derivation of TSRs. Determining the adequacy of safety management program characteristics entails being able to conclude that the DSA contains sufficient documentation and basis to arrive at the following conclusions:

- The major programs needed to provide programmatic safety management are identified.
- Basic provisions of identified programs are noted and references to facility or site program documentation are provided.

The acceptance of safety management program characteristics does not constitute acceptance of the adequacy of program compliance with DOE directives. That can only be accomplished by detailed compliance review of each of the programs, which is beyond the scope of a DSA.

APPROVAL BASIS FOR TECHNICAL SAFETY REQUIREMENTS

NNSA reviews of TSRs are conducted in coordination with DSA reviews, and by many of the same team members. The management plan should address DSA and TSR reviews. Approvals and implementation of the DSA and TSRs must be coordinated because the TSRs must implement commitments made in the DSA.

Approval Basis

The approval bases for the TSR document are the TSR provisions. These TSR provisions may be design features, SLs, OLs, SRs, or ACs. The approval basis for a TSR document includes a disciplined analysis of hazard controls. Determining the adequacy of the TSR provisions entails being able to conclude that

- hazard controls discussed in the DSA are faithfully translated into TSR provisions, and
- the TSR provisions are appropriate and consistent with the DSA.

The sources of information in a DSA regarding these provisions are:

- the hazards analysis, including the description of hazard controls;
- the description of SSCs, the classification of these SSCs as safety-class, safety significant, or other important defense-in-depth SSCs;
- the description of the functional requirements for the safety SSCs;
- the derivation of TSRs section; and

- the descriptions of the safety management programs.

Hazards Analysis

A hazards analysis will include a disciplined analysis of all hazards within the scope of the DSA, including a listing of applicable preventive and mitigative hazard controls. These controls may include safety SSCs, design features, and provisions of various safety management programs. These controls should be regarded as DSA commitments. They should be traced through DSA documentation to specific TSR provisions.

Safety SSC

Safety SSCs must be described in sufficient detail in a DSA so that their functional requirements are defined and the bases for TSR requirements are derived. These safety SSCs will be either active or passive. If passive, they should also be considered for designation as design features in the TSR. These are features of facility design that may not be changed without NNSA review and approval. A crosscheck between DSA-identified important design features and the design features section of the TSR should be conducted to ensure consistency. If active, safety-class SSCs will usually have a SL, a LCS, and a SR associated with it. An active safety-significant SSC may have a LCO and SR and/or specific provisions of a maintenance management program associated with it. In any case, safety SSCs must be addressed specifically in TSR provisions. Technical bases for LCSs and SRs in the basis appendix of the TSR should be reviewed for adequacy. All these provisions are directed at assurance that the safety function of the SSC will be protected.

SAFETY EVALUATION REPORTS

The review process results in the generation of a SER that is integral to the facility's authorization basis. The SER for a given facility or operation documents

- that an appropriate review of the DSA and TSRs was conducted, and
- the basis for approving these documents and any conditions of approval.

Approval signifies that NNSA has accepted these documents as appropriately documenting the safety basis of a facility and as serving as the bass for operational controls that are necessary to maintain an acceptable operating envelope. The SER is developed specifically to document acceptance of the DSA and TSRs. Therefore, significant issues concerning these documents are typically resolved and incorporated in the DSA and TSRs before the final SER is prepared. Only statements pertinent to accepting the facility basis are included in the SER. In accomplishing this, informed judgment and discretion are used to focus the SER on facts that clearly reflect the actual conditions of the facility safety basis. The SER does not need to repeat in wholesale fashion material contained in the DSA and TSRs. The SER provides an overall summary of the methods, assumptions, bases, conclusions, and commitments in the DSA and TSRs.

The SER clearly states any conditions of approval that impose additional commitments to which facility management must adhere beyond those already documented in the DSA and TSRs. Conditions that could be incorporated into the body of these documents are so incorporated during the review process and issue resolution. However, if necessary, the approval authority can expedite approval by defining specific conditions of approval in the SER without requiring revision of the DSA and TSRs.

Approval statements addressing specific areas of the safety basis are augmented with brief summaries of the most significant facility-specific points in those areas to provide a basic context to understand what is being approved. In stating the adequacy of the approval basis, it may also prove advantageous and/or warranted for the SER to discuss areas of concern or issues with significant ramifications for facility operations. Generally, these issues are resolved and any inquiries into them are completed during the review process. Any discussion of issues in the SER should be on a summary level and directed towards clarifying some specific aspect of approval or demonstrating understanding of some aspect of the facility safety basis.

If the SER imposes a condition of approval on the facility safety basis documented in the DSA and TSRs, the SER modifies that facility safety basis. In such cases, conditions cited in the SER become part of the facility safety basis. Therefore, a facility safety basis is composed of an approved DSA and TSRs modified as necessary by the SER to reflect NNSA-imposed conditions of authorization. The SER or memorandum stating the conditions is subsequently appended to the DSA and TSRs.

Note: You do not have to do Example 4 on the following page, but it is a good time to

check your skill and knowledge of the information covered. You may do Example 3 or go directly to the practice.

EXAMPLE 4

1. State the purpose of a USQ.

2. State the purpose of a SER.

3. List the sources of information in a DSA.

Note: When you are finished, compare your answers to those contained in the Example 4 Self-Check. When you are satisfied with your answers, go on to the practice.

EXAMPLE 4 SELF-CHECK

1. State the purpose of a USQ.
   The USQ process allows contractors to make physical and procedural changes and to conduct tests and experiments without prior NNSA approval if the proposed change can be accommodated within the existing safety basis.

2. State the purpose of a SER.
   The SER for a given facility or operation documents that an appropriate review of the DSA and TSRs was conducted, and the basis for approving these documents and any conditions of approval.

3. List the sources of information in a DSA.
   The sources of information in a DSA regarding these provisions are:
   - the hazards analysis, including the description of hazard controls;
   - the description of SSCs, the classification of these SSCs as safety-class, safety significant, or other important defense-in-depth SSCs;
   - the description of the functional requirements for the safety SSCs;
   - the derivation of TSRs section; and
   - the descriptions of the safety management programs.

Change No: 0 Safety Basis Documents Level: Familiar Date: 10/15/03

PRACTICE

This practice is required if your proficiency is to be verified at the familiar level. The practice will prepare you for the criterion test. You will need to refer to the resources to answer the questions in the practice correctly. The practice and criterion test will also challenge additional analytical skills that you have acquired in other formal and on-the-job training.

PRACTICE

1. State the intent of safety basis requirements.

2. Describe the situations in which a contractor must implement a USQ procedure.

3. State the safe harbor method for preparing a DSA for transportation activities.

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

4. Discuss the purpose of a DSA.

5. Discuss the purpose of LCSs.

6. State the four circumstances that result in a violation of a TSR.

7. Discuss the conditions in which a change involves a USQ.

8. Discuss the steps that should be included in a change control process.

9. Discuss the basic components of a DSA review plan.

Change No: 0
Safety Basis
Documents
Level: Familiar
Date: 10/15/03

10. Define the term “significant issue.”

Note: The course manager will check your practice and verify your success at the familiar level. When you have successfully completed this practice, go to the General Level module.

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

SAFETY BASIS DOCUMENTS
GENERAL LEVEL

OBJECTIVES

Given the familiar level of this module, a scenario, and an analysis, you will be able to:

1. list the key elements you would look for in the contractor's action plan to correct the situation described in the scenario; and

2. state which requirements, sections, or elements of the resources for this module apply to the situation described in the scenario.

Note: If you think that you can complete the practice at the end of this level without working through the instructional material and/or the examples, complete the practice now. The course manager will check your work. You will need to complete the practice in this level successfully before taking the criterion test.

Change No: 0 Safety Basis Documents Level: General Date: 10/1/03

RESOURCES

10 CFR 830, "Nuclear Safety Management, Subpart B, Safety Basis Requirements"
DOE G 421.1-2, *Implementation Guide for Use in Developing Documented Safety Analyses to Meet Subpart B of 10 CFR 830*
DOE G 423.1.1, *Implementation Guide for Use in Developing Technical Safety Requirements*
DOE G 424.1-1, *Implementation Guide for Use in Addressing Unreviewed Safety Question Requirements*
DOE-STD-1104-96, *Review and Approval of Nuclear Facility Safety Basis Documents (Documented Safety Analyses and Technical Safety Requirements)*

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

INTRODUCTION

The familiar level of this module included the safety documents that comprise the safety basis for a nuclear facility. The example scenario includes a situation, the actions taken to remedy the situation, and the requirements related to the situation. Students will be asked to review the contractor's actions and decide if they are correct. Students will also be asked to decide if the correct requirements were cited in each situation. Please refer to the resources to make your analysis and answer the questions. You are not required to complete the example. However, doing so will help prepare you for the criterion test.

Note: You do not have to do the example on the following page, but it is a good time to check your skill and knowledge of the information covered. You may do the example or go on to the practice.

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

EXAMPLE SCENARIO

Please review the following scenario and then state if a USQ exists. Support your answer with information contained in the resources.

SCENARIO

A maintenance crew was preparing to repair a heating, ventilation, and air conditioning system (HVAC) in Building 707. A diagnosis of the system revealed that a bearing needed to be replaced. The bearing would be replaced with an identical part. This operation was a part of the routine preventive maintenance schedule. The TSR included provisions for allowable outage times, permissible mode conditions, and permitted reduction in redundancy for the HVAC system. The maintenance crew believed they could accomplish the repairs and satisfy all the conditions in the TSR. Facility personnel determined that vital safety systems would be compromised and initiated a USQ determination.

Take some time to review the example scenario and then decide if a USQ exists. Write your answer below and then compare your answer to the one contained in the example self-check.

EXAMPLE SELF-CHECK

Your response regarding whether or not a USQ exists must match the self-check. The supporting information does not have to match exactly, but the justification for your response should be similar.

A USQ does not exist.

A safety evaluation is not required for routine maintenance procedures if allowable outage times, permissible mode conditions, and permitted reductions in redundancy are covered by the TSR. An additional consideration is that the bearing was replaced with an identical part. (DOE G 424.1-1, section 2.1)

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

PRACTICE

This practice is required if your proficiency is to be verified at the general level. If you are to be qualified as a facility representative, the practice will prepare you for the criterion test. You will need to refer to the CFR, guides, and standards listed in the resources to answer the questions in the practice correctly. The practice and the criterion test will also challenge additional analytical skills that you have acquired in other formal and on-the-job training for the facility representative position.

Please review the following scenario, and then answer these questions.

1. Is the contractor's action plan correct? If not, state what should have been done.
2. Were the correct documents or requirements cited? If not, state the correct documents or requirements.

SCENARIO

In October 2002, a safety team determined that a cooling water system presented a potentially inadequate safety analysis (PISA). The PISA is based on a failure of the Basis of Interim Operations (BIO) to consider a coolant bypass flow path that created reduced coolant flow through the systems even though the flow switches indicated full coolant flow.

An investigation of the incident revealed the following.

The target cooling water system is a closed-loop system that provides cooling to the upper tungsten target, the proton beam window and the lower tungsten target components. Cooling water pressure is measured at the pump discharge and again at a location downstream of the coolant. Flow switches on the upper and lower targets serve as the primary safety-significant control by activating the radiation security system (RSS) when they sense low flow. The RSS causes the insertion of beam plugs that block beam to the target. The flow switches are set to activate when flow falls below 8.9 gallons per minute (gpm). The acceptance limit in the 1L target BIO is 6.0 gpm, based on flow required to remove the heat generated by a 150-microampere beam current. The system is normally operated at 11 plus or minus 1 gpm. Flow meters measure the flow through each component in the target cooling system. During the 2001 run cycle, the 1L target was operated at a flow rate of 11 plus or minus 1 gpm, and a beam current that never exceeded 108 miocroamperes. After June of 2002, the upper target flow was again 11 plus or minus 1 gpm and the beam current was 55-60 microamperes.

In October 2002, the safety team leader instituted trending analysis of operational data for the time frame starting at the initial target operation in 1998. Included in the trending analysis were target end-cap temperatures and the relative flow constant across the target. The flow constant, calculated from the measured flow in gpm divided by the square root of the pressure drop, rose from 0.9 to 1.6 between June and August of the 2001 run cycle. The change in the flow factor was not obvious to target operations personnel during the 2001 run cycle since the flow remained constant while the pressure drop decreased. The relative flow constant has been stable since October 2001.

An engineering analysis was completed for the discrepant-as-found condition. Several failure mode models were considered in reference to the operational data and engineering calculations. The team determined that the most likely scenario involved an internal weld failure on the inlet flow plenum of the upper target assembly. Until the target is removed, as scheduled for 2003, the failure mode cannot be confirmed. However, the scenario is consistent with the pressure drop and the accompanying 25 percent increase in temperature to the upper and lower end-caps as indicated by multiple thermocouples. The weld failure would allow a portion of the upper target cooling water to bypass the series of tungsten plates without leaking from the closed loop.

Because the analysis indicates a failure in a weld on the inlet flow plenum, the direct and root cause of the event was identified as an equipment/material problem: defective weld, braze, or soldered joint.

Based on the engineering calculations, the actual flow through the target plates is believed to be 5 gpm. The reduced flow through the plates resulted in the appearance of an inadequate safety analysis that was later rejected because the actual safety margin was not reduced. The safety margin was not compromised because the 2001 and 2002 run cycle beam currents were significantly lower than the approved current limit. At 108 microamperes current, the 6-gpm-acceptance flow rate scales to 4 gpm.

The team completed further reviews of the failure mode in terms of accident scenarios developed in the 1L target BIO. The team determined that the unique design of the upper target and casing provided the only loss-of-coolant accident scenario in which the intended flow path could be bypassed without being immediately detected. The upper target is the only 1L target component made up of a series of plates with cooling chambers running between the plates. The Inconel-718 casing design was based on the target design and consisted of several welds between the plates and the return plenum that do not exist on the casing for the solid lower target. The team reviewed the other target components and determined all other coolant leaks are either already considered in the 1L target BIO or are readily detectable through a compromise of vacuum or other indicators.

Actions taken by the contractor.
The senior safety basis manager implemented the following controls:

- The acceptance limit for the proton beam current on-target was established at 75 microamperes. Based on the margin of error of approximately 4 microamperes due to instrumentation calibration and other causes, a hardware transmission monitor trip-point was set at or below 66 microamperes, providing an operations beam current maximum of 70 microamperes.
- The upper and lower target end-cap maximum temperatures were defined, and the minimum number of thermocouples in each cap was identified. The upper target end-cap maximum allowable temperature was set at 250 degrees Celsius, and the lower end plat maximum allowable temperature was set at 160 degrees Celsius. The temperature is averaged based on a minimum of 2 functioning thermocouples per end-cap.

The team initiated an unreviewed safety question determination and determined that this condition did not constitute a positive USQ as the margin of safety to workers was not reduced.

Requirements related to this scenario.
G 424.1-1, *Implementation Guide for use in Addressing Unreviewed Safety Question Requirements*, requires USQ determinations for changes to a nuclear facility that alter an SSC's design, function, or method of performance as described in the existing safety analyses by text, drawing, or other information relied on as the safety basis. The safety analyses include descriptions of many SSCs, but a nuclear facility also contains many SSCs not explicitly described in the safety analyses. These can be components, subcomponents of larger components, or even entire systems.

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

Take some time to review the scenario and the actions the contractor took or didn't take to correct the situation. Then decide if the contractor's actions were complete and correct. Finally, determine if the requirements, sections, or elements of cited in the scenario were correct.

Write your answers below and then bring the completed practice to the course manager for review.

Change No: 0
Safety Basis
Documents
Level: General
Date: 10/1/03

Note: The course manager will check your practice and verify your success at the General Level. When you have successfully completed this practice, the course manager will give you the criterion test.